U.S. Department of Justice

Richard P. Donoghue
United States Attorney
Eastern District of New York

271 Cadman Plaza East
Brooklyn, New York 11201

FOR IMMEDIATE RELEASE **November 27, 2018**

Contact:
John Marzulli
Tyler Daniels
United States Attorney's Office
(718) 254-6323

PRESS RELEASE

TWO INTERNATIONAL CYBERCRIMINAL RINGS DISMANTLED AND EIGHT DEFENDANTS INDICTED FOR CAUSING TENS OF MILLIONS OF DOLLARS IN LOSSES IN DIGITAL ADVERTISING FRAUD

Global Botnets Shut Down Following Arrests

A 13-count indictment was unsealed today in federal court in Brooklyn charging Aleksandr Zhukov, Boris Timokhin, Mikhail Andreev, Denis Avdeev, Dmitry Novikov, Sergey Ovsyannikov, Aleksandr Isaev and Yevgeniy Timchenko with criminal violations for their involvement in perpetrating widespread digital advertising fraud. The charges include wire fraud, computer intrusion, aggravated identity theft and money laundering. Ovsyannikov was arrested last month in Malaysia; Zhukov was arrested earlier this month in Bulgaria; and Timchenko was arrested earlier this month in Estonia, all pursuant to provisional arrest warrants issued at the request of the United States. They await extradition. The remaining defendants are at large.

Also unsealed today in federal court in Brooklyn were seizure warrants authorizing the FBI to take control of 31 internet domains, and search warrants authorizing the FBI to take information from 89 computer servers, that were all part of the infrastructure for botnets engaged in digital advertising fraud activity. The FBI, working with private sector partners, redirected the internet traffic going to the domains (an action known as "sinkholing") in order to disrupt and dismantle these botnets.

Richard P. Donoghue, United States Attorney for the Eastern District of New York, William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), and James P. O'Neill, Commissioner, New York City Police Department (NYPD) announced the charges and domain seizures.

"As alleged in court filings, the defendants in this case used sophisticated computer programming and infrastructure around the world to exploit the digital advertising industry through fraud," stated United States Attorney Donoghue. "This case sends a powerful

message that this Office, together with our law enforcement partners, will use all our available resources to target and dismantle these costly schemes and bring their perpetrators to justice, wherever they are." Mr. Donoghue thanked the FBI Cyber Division for its extraordinary efforts in carrying out the multi-year investigation.

"As alleged, these individuals built complex, fraudulent digital advertising infrastructure for the express purpose of misleading and defrauding companies who believed they were acting in good faith, and costing them millions of dollars. This kind of exploitation undermines confidence in the system, on the part of both companies and their customers," stated FBI Assistant Director-in-Charge Sweeney. "Thanks to the hard work of our legal attachés and law enforcement partners overseas, with the cooperation of our international and U.S.-based private sector partners, the defendants will face justice for their alleged crimes."

"This investigation highlights public- and private-sector collaboration across the globe, and again confirms the absolute necessity for interagency information-sharing. Criminals – especially those operating via the internet – do not concern themselves with jurisdictional boundaries, so it is critical that the law-enforcement community works together to achieve our shared goal of protecting the people we serve," stated NYPD Commissioner O'Neill. "I thank and commend the U.S. Attorney for the Eastern District, and all the investigators with the FBI Cyber Division and the NYPD. Together, we are ensuring that the vital systems and technologies of our economy are kept safe."

The Criminal Scheme

The internet is, in large part, freely available to users worldwide because it runs on digital advertising: website owners display advertisements on their sites and are compensated for doing so by intermediaries representing businesses seeking to advertise their goods and services to real human customers. In general, digital advertising revenue is based on how many users click or view the ads on those websites. As alleged in court filings, the defendants in this case represented to others that they ran legitimate companies that delivered advertisements to real human internet users accessing real internet webpages. In fact, the defendants faked both the users and the webpages: they programmed computers they controlled to load advertisements on fabricated webpages, via an automated program, in order to fraudulently obtain digital advertising revenue.

The Datacenter-Based Scheme (Methbot)

As alleged in the indictment, between September 2014 and December 2016, Zhukov, Timokhin, Andreev, Avdeev and Novikov operated a purported advertising network ("Ad Network #1") and, with Ovsyannikov's assistance, carried out a digital ad fraud scheme. Ad Network #1 had business arrangements with other advertising networks whereby it received payments in return for placing advertising placeholders ("ad tags") on websites. Rather than place these ad tags on real publishers' websites, however, Ad Network #1 rented more than 1,900 computer servers housed in commercial datacenters in Dallas, Texas and elsewhere, and used those datacenter servers to load ads on fabricated websites, "spoofing" more than 5,000 domains. To create the illusion that real human internet users were viewing the advertisements loaded onto these fabricated websites, the defendants programmed the datacenter servers to

simulate the internet activity of human internet users: browsing the internet through a fake browser, using a fake mouse to move around and scroll down a webpage, starting and stopping a video player midway, and falsely appearing to be signed into Facebook. Furthermore, the defendants leased more than 650,000 Internet Protocol ("IP") addresses, assigned multiple IP addresses to each datacenter server, and then fraudulently registered those IP addresses to make it appear that that the datacenter servers were residential computers belonging to individual human internet users who were subscribed to various residential internet service providers. As a result of this scheme, Ad Network #1 falsified billions of ad views and caused businesses to pay more than $7 million for ads that were never actually viewed by real human internet users.

The Botnet-Based Scheme (3ve.2 Template A)

As also alleged in the indictment, between December 2015 and October 2018, Ovsyannikov, Timchenko and Isaev operated a purported advertising network ("Ad Network #2") and carried out another digital ad fraud scheme. In this scheme, the defendants used a global "botnet"—a network of malware-infected computers operated without the true owner's knowledge or consent—to perpetrate their fraud. The defendants developed an intricate infrastructure of command-and-control servers to direct and monitor the infected computers and check whether a particular infected computer had been flagged by cybersecurity companies as associated with fraud. By using this infrastructure, the defendants accessed more than 1.7 million infected computers, belonging to ordinary individuals and businesses in the United States and elsewhere, and used hidden browsers on those infected computers to download fabricated webpages and load ads onto those fabricated webpages. Meanwhile, the owners of the infected computers were unaware that this process was running in the background on their computers. As a result of this scheme, Ad Network #2 falsified billions of ad views and caused businesses to pay more than $29 million for ads that were never actually viewed by real human internet users.

The Botnet Takedown

Following the arrest of Ovsyannikov by Malaysian authorities, U.S. law enforcement authorities, in conjunction with various private sector companies, began the process of dismantling the criminal cyber infrastructure utilized in the botnet-based scheme, which involved computers infected with malicious software known in the cybersecurity community as "Kovter." The FBI executed seizure warrants to sinkhole 23 internet domains used to further the charged botnet-based scheme or otherwise used to further the Kovter botnet. The FBI also executed search warrants at 11 different U.S. server providers for 89 servers related to the charged botnet-based scheme or Kovter.

In addition, as part of its investigation, the FBI discovered an additional cybercrime infrastructure committing digital advertising fraud through the use of datacenter servers located in Germany and a botnet of computers in the United States infected with malicious software known in the cybersecurity community as "Boaxxe." The FBI executed seizure warrants to sinkhole eight domains used to further this scheme and thereby disrupt yet another botnet engaged in digital advertising fraud.

Finally, the United States, with the assistance of its foreign partners, executed seizure warrants for multiple international bank accounts in Switzerland and elsewhere that were associated with the schemes.

The charges in the indictment are merely allegations and the defendants are presumed innocent unless and until proven guilty.

The government's case is being prosecuted by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Saritha Komatireddy, Alexander F. Mindlin, Michael T. Keilty and Karin K. Orenstein are in charge of the prosecution.

The Justice Department's Office of International Affairs, the FBI's Legal Attachés abroad and foreign authorities in multiple countries provided critical assistance in this case. The Office extends its appreciation to the Attorney General's Chambers of Malaysia, the Royal Malaysian Police, the Malaysian National Central Bureau of Interpol, the Supreme Cassation Prosecution Office of Bulgaria, the Regional Prosecution Office of Varna, the Cybercrime Department of the Bulgarian General Directorate for Combating Organized Crime, the Bulgarian Ministry of Interior Regional Directorate of Varna, the Office of the Prosecutor General of Estonia, the Estonian Police and Border Guard Board and the FBI's Legal Attaché Offices in Malaysia, Bulgaria and Estonia for their assistance in apprehending defendants in this case. The Office also extends its appreciation to the German Bundeskriminalamt Cybercrime Intelligence Operations Department and Polizei Sachsen Polizeidirektion Zwickau Criminal Investigation Department, the Dutch National Police, the United Kingdom National Crime Agency, the French Police Cybercrime Central Bureau, the Swiss Federal Office of Justice, FBI's Legal Attaché Offices in those countries, and Europol for their assistance in various aspects of the investigation and botnet takedown.

Multiple private sector organizations also provided critical assistance in this case. The Office extends its appreciation to White Ops, Inc. and Google LLC for their assistance in the investigation and botnet takedown. The Office also extends its appreciation to Microsoft Corporation, ESET, Trend Micro Inc., CenturyLink, Inc, F-Secure Corporation, Malwarebytes, MediaMath, the National Cyber-Forensics and Training Alliance and The Shadowserver Foundation for their assistance in the botnet takedown.

For technical details on the malware and botnets referenced in this case, please see US-CERT Alert TA18-331A: https://www.us-cert.gov/ncas/alerts/TA18-331A

The Defendants:

ALEKSANDR ZHUKOV
Age: 38
Russian Federation

BORIS TIMOKHIN
Age: 39
Russian Federation

MIKHAIL ANDREEV
Age: 34
Russian Federation and Ukraine

DENIS AVDEEV
Age: 40
Russian Federation

DMITRY NOVIKOV
Age: Unknown
Russian Federation

SERGEY OVSYANNIKOV
Age: 30
Republic of Kazakhstan

ALEKSANDR ISAEV
Age: 31
Russian Federation

YEVGENIY TIMCHENKO
Age: 30
Republic of Kazakhstan

E.D.N.Y. Docket No. 18-CR-633 (ERK)